AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1. (Currently amended) A method to facilitate locking an adversary out of

2   a network application, comprising:

3   receiving at a server a request, including an authentication credential, to

4   access the network application, wherein the authentication credential includes a

5   user identifier associated with a user and a network address of a user device;

6   examining an audit log to determine if the user identifier has been locked

7   out from the network address; and

8   if the user identifier has been locked out from the network address,

9   denying access to the network application;

10   otherwise, checking the authentication credential for validity, and

11   if the authentication credential is valid,

12   allowing access to the network application,

13   otherwise,

14   logging a failed attempt in the audit log, wherein the

15   user identifier is locked out from the network address after

16   a threshold number of failed attempts,

17   <u>imposing a global lockout for the user identifier</u>

18   <u>after a threshold number of network addresses are locked</u>

19   <u>out for the user identifier,</u> and

20   denying access to the network application;

21   whereby the adversary is prevented from accomplishing an attack by

22   masquerading as the user.

1   2 (Canceled).

1   3. (Currently amended) The method of ~~claim 2~~claim 1, further comprising:

2   removing ~~comprising removing~~ a lockout after a predetermined period of time.

1   4. (Currently amended) The method of ~~claim 2~~claim 1, further comprising:

2   manually ~~comprising manually~~ removing a lockout by an administrator of the

3   server.

1   5. (Original) The method of claim 1, wherein the authentication credential

2   includes a user name and a password.

1   6. (Original) The method of claim 5, wherein checking the authentication

2   credential for validity involves:

3   verifying that an administrator has authorized access to the network

4   application for a combination of the user name and the password; and

5   determining if the request violates an access rule in a rule table.

1   7. (Original) The method of claim 6, wherein the access rule can specify:

2   an allowed time-of-day;

3   an allowed number of access attempts;

4   an allowed network address; and

5   an allowed network domain.

1   8. (Original) The method of claim 1, wherein the network address includes

2   an Internet Protocol address.

1   9. (Currently amended) A computer-readable storage medium storing

2   instructions that when executed by a computer cause the computer to perform a

3   method to facilitate locking an adversary out of a network application,

4   comprising:

5   receiving at a server a request, including an authentication credential, to

6   access the network application, wherein the authentication credential includes a

7   user identifier associated with a user and a network address of a user device;

8   examining an audit log to determine if the user identifier has been locked

9   out from the network address; and

10   if the user identifier has been locked out from the network address,

11   denying access to the network application;

12   otherwise, checking the authentication credential for validity, and

13   if the authentication credential is valid,

14   allowing access to the network application,

15   otherwise,

16   logging a failed attempt in the audit log, wherein the

17   user identifier is locked out from the network address after

18   a threshold number of failed attempts,

19   imposing a global lockout for the user identifier

20   after a threshold number of network addresses are locked

21   out for the user identifier, and

22   denying access to the network application;

23   whereby the adversary is prevented from accomplishing an attack by

24   masquerading as the user.

1   10 (Canceled).

1   11. (Currently amended) The computer-readable storage medium of ~~claim~~
2   ~~10~~claim 9, the method further <u>comprising: removing</u> ~~comprising removing~~ a
3   lockout after a predetermined period of time.

1   12. (Currently amended) The computer-readable storage medium of ~~claim~~
2   ~~10~~claim 9, the method further <u>comprising: manually</u> ~~comprising manually~~
3   removing a lockout by an administrator of the server.

1   13. (Original) The computer-readable storage medium of claim 9, wherein
2   the authentication credential includes a user name and a password.

1   14. (Original) The computer-readable storage medium of claim 13,
2   wherein checking the authentication credential for validity involves:
3   verifying that an administrator has authorized access to the network
4   application for a combination of the user name and the password; and
5   determining if the request violates an access rule in a rule table.

1   15. (Original) The computer-readable storage medium of claim 14,
2   wherein the access rule can specify:
3   an allowed time-of-day;
4   an allowed number of access attempts;
5   an allowed network address; and
6   an allowed network domain.

1   16. (Original) The computer-readable storage medium of claim 9, wherein
2   the network address includes an Internet Protocol address.

1   17. (Currently amended) An apparatus to facilitate locking an adversary

2   out of a network application, comprising:

3   a receiving mechanism that is configured to receive at a server a request,

4   including an authentication credential, to access the network application, wherein

5   the authentication credential includes a user identifier associated with a user and a

6   network address of a user device;

7   an examining mechanism that is configured to examine an audit log to

8   determine if the user identifier has been locked out from the network address; and

9   an access mechanism that is configured to deny access to the user

10   identifier if the user identifier has been locked out from the network address;

11   a validation mechanism that is configured to check the authentication

12   credential for validity, wherein the access mechanism is further configured to

13   allow access if the authentication credential is valid; ~~and~~

14   a logging mechanism that is configured to log a failed attempt in the audit

15   log, wherein the user identifier is locked out from the network address after a

16   threshold number of failed attempts, and wherein the access mechanism is further

17   configured to deny access to the user identifier after a failed access attempt;

18   <u>a lockout mechanism that is configured to impose a global lockout for the</u>

19   <u>user identifier after a threshold number of network addresses are locked out for</u>

20   <u>the user identifier; and</u>

21   whereby the adversary is prevented from accomplishing an attack by

22   masquerading as the user.

1   18 (Canceled).

1   19. (Currently amended) The apparatus of ~~claim 18~~<u>claim 17</u>, further

2   <u>comprising: a</u> ~~comprising a~~ lockout removing mechanism that is configured to

3   remove a lockout after a predetermined period of time.

6

1 20. (Currently amended) The apparatus of ~~claim 18~~claim 17, further

2 comprising: a ~~comprising a~~ lockout removing mechanism that is configured to

3 allow an administrator of the server to manually remove a lockout.

1 21. (Original) The apparatus of claim 17, wherein the authentication

2 credential includes a user name and a password.

1 22. (Original) The apparatus of claim 21, further comprising:

2 a verification mechanism that is configured to verify that an administrator

3 has authorized access to the network application for a combination of the user

4 name and the password; and

5 a violation determining mechanism that is configured to determine if the

6 request violates an access rule in a rule table.

1 23. (Original) The apparatus of claim 22, wherein the access rule can

2 specify:

3 an allowed time-of-day;

4 an allowed number of access attempts;

5 an allowed network address; and

6 an allowed network domain.

1 24. (Original) The apparatus of claim 17, wherein the network address

2 includes an Internet Protocol address.